PATENT
Attorney Docket No. P3166US
(Formerly 5284-55PUS)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Allain, et al.

Application No. 10/529,989

Group Art Unit: 2431

Examiner: Longbit Chai

Filed: October 20, 2005

For: METHOD AND INSTALLATION FOR CONTROLLING A TELEPHONE CALL TRANSMITTER ON AN INTERNET NETWORK AND TELEPHONE TERMINAL THEREFOR

REQUEST FOR PRE-APPEAL BRIEF CONFERENCE

Mail Stop AF
Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

The Applicants thank the Examiner for his courtesy and diligent efforts during the prosecution of this application and helpful and constructive comments made during the telephone interview.

The Applicants respectfully request a pre-appeal brief conference pursuant to the U.S.P.T.O. Official Gazette Notice "New Pre-Appeal Brief Conference Pilot Program" dated 12 July 2005, as extended by the U.S.P.T.O. Official Gazette Notice "Extension of the Pilot Pre-Appeal Brief Conference Program" dated 07 February 2006. As required by this procedure, Applicants are herewith providing, in five or less total pages, a succinct, concise and focused set of arguments for which the review is being requested.

The Applicants submit that the present request is proper because, in the view of the Applicants, the final rejection is founded upon clear legal and factual deficiencies rather than presenting an issue based upon a subjective interpretation of the claims or prior art teachings. The Applicants assert that clear error exists in the Examiner's final rejection of independent claims 1 and 11 under 35 U.S.C. § 102(e) as anticipated by U.S. Patent Publication No. 2003/0097584 ("Haukka").

In sum, it is the Applicants' position that Haukka fails to teach or suggest the claimed decrypting element.

Examiner's Position

In the Final Office Action, on pp. 4–5, the Examiner asserted, among other things, that Haukka teaches the claimed decrypting element as follows:

> **a remote call management server decrypting the control code** (Haukka: Figure 2 & Para [0009] Line[s] 1–4 / Line[s] 8–9; Para [0023] Line[s] 5–7 and Para [0017] Line[s] 23–26; P-CSCF is a proxy server;
>
> **comparing at least one parameter extracted from the decrypted control code with corresponding information stored in a database hosted in the server** (Haukka: Para [0017] Line[s] 32–35; the temporary identity index (control code) is stored in a database of the visiting network);

In the Advisory Action, the Examiner states, under section 2(a)(ii) that:

> the temporary identity index [which is a hash function of an encrypted public identity of the user equipment UE 10] is created and placed into a[n] SIP message which is then encrypted, before the transmission, using an encryption algorithm determined during the registration of the UE (Haukka: Para [0009] Line[s] 1–9)...

During the telephone interview, the Examiner further raised the possibility that Haukka's alternate embodiment disclosed in ¶¶ 0010, 0022, and 0023 related to the URI could alternately disclose the present invention in that the URI could further be read on the claimed control code.

Applicants' Position

Claim 1 requires, "decrypting, at a remote call management server, the encrypted control code". Applicants do not see such a claimed step in Haukka, and understand that this is because Haukka relies on hash values which cannot be decrypted.

The Examiner has equated the claimed control code with Haukka's temporary identity index. This temporary identity index contains information associated with the public identity of the User Equipment (UE). However, as stated at 0017:24–27 (paragraph : lines):

> [the P-CSCF and UE] then calculate a temporary identity index using a hash function Hk(x), where x is a public identity of the UE 10, and k is one of the private keys CK and IK.

The Examiner stated in his Advisory Action regarding argument (a)(ii):

> Haukka teaches... [t]he temporary identity index is created and placed into a SIP message which is then encrypted, before the transmission...

This is not entirely correct. The temporary identity index is not actually placed in the SIP message that is subsequently encrypted—the temporary identity index is placed in a header of the encrypted SIP message, and not the encrypted part of the SIP message itself. The header itself is not encrypted (as it would be if it was a part of the SIP message). As Haukka states at 0009:1–6, 12–14:

> Once the temporary identity index is created, it may be inserted into a header of the message. For example, the temporary identity index may be inserted into a call-info header field of a session initiation protocol (SIP) message in place of a request Uniform Resource Identifier (URI) for providing the sender's identity.
>
> ...another line including a call-info header filed [is] added to the encrypted SIP message.

Indeed, as explained in Haukka at 0005:18–21:

> Accordingly, an SIP message is encrypted in SIP-level by splitting the message to be sent into a part to be encrypted and a short header that remains clear, i.e., not encrypted.

So, in paraphrasing Haukka slightly, Haukka teaches the inclusion of the hash value as a temporary identity index that is inserted into the normally non-encrypted/clear header portion of the SIP message *after* the SIP message is encrypted (see Haukka 0021:2–7)—i.e., it is not encrypted as a part of the SIP message and is inserted after the encryption of the SIP message. Therefore, whatever decrypting occurs in Haukka in order to get at the message contents does not occur with regard to the temporary identity index.

Instead, since one of ordinary skill in the art knows that a hash value (which is what the temporary identity index is) by its nature cannot be decrypted, the mechanism that both the requestor and requestee use is to both calculate a hash value and then compare them. Therefore, if the Examiner is taking the position that the temporary identity index, created as a hash value, reads on the claimed encrypted control code (i.e., that this is an encryption), then Figure 2 of Haukka shows that both the requestor and requestee are *both encrypting*, since the exact same function is being shown in the bottom box of Figure 2, and does not

show encrypting *and decrypting*, as required by the claims. Haukka does not decrypt the temporary identity index nor does it have to for any purpose.

Additionally, it would make no sense to further encrypt the hash value of the encrypted public identity of the UE, since the stated purpose in Haukka of maintaining confidentiality of the sender is fully realized by hashing the sender's public identity and performing a further encryption would waste processing power without providing any further benefit.

Regarding the possible interpretation discussed with the Examiner during the telephone interview that Haukka's URI could alternately read on the claimed control code, Applicants respectfully assert that such an interpretation is not viable.

Haukka provides an improvement over a traditional "Reverse DNS Look-up". In this traditional method, a mail server, after receiving some message, looks up the URI (e.g., viz., the IP address) of the sender as displayed in the message header. This URI is then compared to knowledge about the URI of the sender coming from another source (typically on the basis of a statement contained in the message itself). If the two URI's do not match, the message is rejected. Thus, it is not possible for a hacker to copy a *legitimate* message previously sent from a first URI, and send this copied message from a second URI.

However, this traditional method is sensitive to the following attack: a hacker could make-up an *illegitimate* message in which the stated first URI would be replaced by a stated second URI. When this illegitimate message is sent from the second URI, the receiving mail server is deceived when implementing the "Reverse DNS Look-Up" method.

Haukka addresses this possibility and provides protection against such an attack with its improved "Reverse DNS Look-up" in which the stated URI is encrypted using an algorithm and secret key known both to sender and receiver. Thus, a hacker will not be able to insert an encrypted second URI since the hacker does not know the encryption algorithm/key.

Haukka's first embodiment for his confidentiality protection method, which the Examiner used as a basis for rejection in the Final Office Action, includes only the call-info header containing the temporary identity index (Fig. 3, step 540) in the entire message, whereas in Haukka's second embodiment, which the Examiner considered during the telephone interview, includes both the call-info header containing the temporary identity index *and* the

encrypted URI (Fig. 4, step 545). Indeed, the identity of the telecommunications terminal (as claimed in claim 1) on one hand, and a URI from where the message was sent on the other hand, represent two separate and distinct elements that are used for different purposes: for example, when a terminal moves from a local network to another local network, this terminal keeps the same identity ("MAC address") but it does not keep its local IP address (assigned by the gateway of each local network).

Although Haukka is silent on the subsequent handling of the URI (and on this basis alone, Haukka does not provide a teaching that would support an interpretation of the URI being used as the claimed control code), any presumed handling of a decrypted URI would of necessity involve comparing it to corresponding information displayed in the header of the received message, which cannot in any way be construed as "a database hosted in the server" (as required by claim 1).

For all the reasons given above and previously argued during prosecution of the application, Applicants respectfully submit that all claims patentably distinguish over the applied art of record, and it is respectfully requested that the rejections be withdrawn and all claims be allowed.

Respectfully submitted,

/jasmine r. patel/

Brian C. Rupp, Reg. No. 35,665
Mark Bergner, Reg. No. 45,877
Jasmine R. Patel, Reg. No. 59,344
DRINKER BIDDLE & REATH LLP
191 N. Wacker Drive, Suite 3700
Chicago, Illinois 60606-1698
(312) 569-1000 (telephone)
(312) 569-3000 (facsimile)
Customer No.: 08968

Date: June 25, 2009